AMENDMENTS TO THE DRAWINGS

The attached replacement sheets of drawings include changes to Figures 1-2. These sheets, which include Figures 1-2, replace the original sheets including Figures 1-2. In both of the figures, the notation "Prior Art" has been added next to the figure number.

Attachment: Replacement Sheets

RECEIVED
CENTRAL FAX CENTER
MAR 0 7 2008

REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-26 are pending in the application. The Examiner additionally stated that claims 1-26 are rejected. By this communication, claim 16 is cancelled and claims 1, 6-8, 17, 20-23, and 26 are amended. Hence, claims 1-15 and 17-26 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Drawings

Applicant has amended the drawings to note that FIGURES 1-2 are prior art.

In the Specification

Paragraph [0012] is hereby amended to remove the hyperlink to the NIST website. In addition, Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-26 under 35 U.S.C. 103(a) as being unpatentable over Yup, US2002/0191784 (hereinafter, "Yup") in view of Dhir et al., US2005/0084076 (hereinafter, "Dhir"). Applicant respectfully traverses the Examiner's rejections.

As per claim 1, the Examiner noted that Yup disclose an apparatus for performing cryptographic operations, comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of said one of the cryptographic operations [page 3, paragraph 0028];

PAGE 15/29 * RCVD AT 3/7/2008 11:10:00 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-5/39 * DNIS:2738300 * CSID:661 460 1986 * DURATION (mm-ss):07-34

- keygen logic (key expansion block), operatively coupled to said cryptographic instruction, configured to direct said computing device to expand said provided cryptographic key into said corresponding key schedule [page 3, paragraph 0028]; and
- execution logic (key expansion logic), operatively coupled to said keygen logic, configured to expand said provided cryptographic key into said corresponding key schedule [page 3, paragraph 0028].

The Examiner conceded that Yup does not explicitly disclose performing these instructions on a microprocessor based platform nor performing the instruction within a single microprocessor.

Nonetheless, the Examiner opined that Dhir discloses a similar apparatus and further discloses performing cryptographic instructions (i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform (i.e., FPGA) [page 5, paragraph 0051].

The Examiner furthermore remarked that Yu discloses a similar apparatus and furthermore discloses performing cryptographic instructions *(i.e., executes several steps of an algorithm)* to implement the Advanced Encryption Standard algorithm on a single microprocessor *(i.e., optimized cipher subprocessor 700)* [column 4, lines 14-30 & figure 7a].

Therefore, the Examiner concluded that it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a single microprocessor, a microprocessor based platform, or any other platform in order to meet particular design requirements.

In addition, the Examiner stated that Applicant argues that Yup does not disclose cryptographic instructions, but the Examiner respectfully disagreed and submitted that while the exact term "cryptographic instructions" is not disclosed, Yup does in fact teach cryptographic instructions (i.e., finite state machine controllers which control the operation of the remaining portions of the circuit) [page 3, paragraph 0025].

Furthermore, the Examiner noted that Applicant argued that neither Yup nor Dhir disclose performing cryptographic operations/instructions within a single microprocessor, yet the Examiner submitted that this is moot in view of the new ground of rejection.

Moreover, the Examiner stated that Applicant argued that neither Yup nor Dhir disclose keygen logic coupled to a cryptographic instruction, configured to expand a provided cryptographic key into a corresponding key schedule. However, the Examiner respectfully disagreed and submitted that Yup does disclose this feature (i.e., under control of its respective FSM, each system channel transmits the stored cipher key to a key expansion block, the key expansion block then generates round keys used for each AES round, these round keys can be viewed as the "key schedule") [page 3, paragraph 0028].

In reply, Applicant respectfully disagrees with the Examiner's characterizations of Yup, Dhir, and Yu vis-à-vis that subject matter which is recited in claim 1. To aid in the following analysis, claim 1, as amended herein, is repeated below.

1. An apparatus for performing cryptographic operations, comprising:

fetch logic, disposed within a microprocessor, configured to receive a single atomic cryptographic instruction as part of an instruction flow executing on said microprocessor, wherein said single atomic cryptographic instruction prescribes one of the cryptographic operations, and wherein said single atomic cryptographic instruction prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of said one of the cryptographic operations;

translation logic, coupled to said fetch logic, configured to translate said single atomic cryptographic instruction into a sequence of micro instructions that directs said microprocessor to perform said one of the cryptographic operations;

keygen logic, disposed within said microprocessor and operatively coupled to said single atomic cryptographic instruction, configured to direct said microprocessor to expand said provided cryptographic key into said corresponding key schedule; and

execution logic, disposed within said microprocessor and operatively coupled to said keygen logic, configured to expand said provided cryptographic key into said corresponding key schedule, said execution logic comprising:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

Applicant has amended claim 1 to recite a "single atomic cryptographic instruction" that prescribes the listed operations. This amendment is provided to more clearly distinguish the present invention over the circuits and "processors" taught by Yup and Yu and support for use of the single atomic cryptographic instruction in a program being executed by a microprocessor may be found in paragraphs 45, 47, 50-51, 54, 102, and 103, *inter alia,* of the instant specification.

Applicant has also amended claim 1 to recite that the execution logic (a logical stage in a microprocessor) comprises a cryptography unit that performed the cryptographic rounds. Numerous paragraphs and figures in the instant disclosure provide support for this amendment and teach that the cryptography unit is one of a plurality of units (e.g., integer unit, floating point unit, MMX unit, SSE unit, etc) in the execution stage of the microprocessor.

Applicant has further amended claim 1 to recite translation logic that translates the single atomic cryptographic instruction into a sequence of micro instructions that directs the microprocessor to perform the one of the cryptographic operations.

In view of these amendments, Applicant respectfully asserts that Yup does not teach use of a single atomic cryptographic instruction to prescribe the operations recited in the

claim. In fact, Applicant has been careful to search Yup and reports that the term "cryptographic instruction" cannot be found. In reply to the Examiner's point that Yup does in fact teach cryptographic instructions (i.e., finite state machine controllers which controls the operation of the remaining portions of the circuit) [page 3, paragraph 0025], Applicant responds that the instant disclosure clearly teaches the meaning of an "instruction" such that it is quite distinct from a finite state machine controller as is taught by Yup in the cited section. The instant disclosure teaches that an instruction, such as the single atomic cryptographic instruction recited in claim 1, is part of an application program. Clearly, a finite state machine controller is not part of an application program. As one skilled in the art will appreciate, a application program's instructions are fetched from memory for execution by a microprocessor. These features of the present invention are not taught or suggested by Yup.

In contrast, Yup teaches "A circuit includes a single circuit portion for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels. The circuit portion includes a circuit for individually generating, on the fly, the round keys used during each round of the AES block cipher algorithm. The circuit portion also includes shared logic circuits that implement the transformations used to encrypt and decrypt data blocks according to the AES block cipher. The single circuit portion encrypts or decrypts data blocks from each of the plurality of system channels in turn, in round-robin fashion. The circuit portion also includes a circuit for determining S-box values for the AES block cipher algorithm. The circuit additionally implements an efficient method for generating round keys on the fly for the AES block cipher decryption process. (Abstract)

Without a doubt, Yup teaches a circuit for implementing the AES block cipher algorithm in a system having a plurality of channels. This is somewhat analogous to prior art stand-alone cryptographic processing units, the problems of which the present inventors have noted and for which the present invention is provided to overcome. Yet, Yup is utterly silent with regard to how the invention is commanded to process data blocks other than to present a plurality of input registers 102 and associated control signals 103 that are coupled to a corresponding plurality of "system channels."

One skilled will appreciate that this type of configuration is cumbersome in that to provide for encryption and/or decryption of data, a processor must provide for communication with Yup's device via some system channel mechanism.

In stark contrast, claim 1 recites a single atomic cryptographic instruction that is fetched from memory by a microprocessor as part of an instruction flow executing on said microprocessor. The claim continues to recited how the single atomic cryptographic instruction prescribes one of a plurality of key sizes. The claim further recites that translation logic translates it into a sequence of micro instructions that direct the microprocessor to perform the one of the cryptographic operations. Yup does not teach or suggest an instruction that provides for the foregoing limitations. The claim also recites keygen logic, disposed within said microprocessor and operatively coupled to said single atomic cryptographic instruction, configured to direct said microprocessor to expand said provided cryptographic key into said corresponding key schedule. The claim additionally recites execution logic that is within the microprocessor as well and that is operatively coupled to said keygen logic, configured to expand said provided cryptographic key into said corresponding key schedule. Although Yup teaches a key expansion block, as the Examiner suggests, such a block is not operatively coupled to a single atomic cryptographic instruction that is fetched from memory as part of an instruction flow, for Yup is silent in this regard.

In addition, claim 1 recites that the cryptographic rounds are performed by a cryptography unit within the execution logic of the microprocessor. Applicant submits that the operations performed by the cryptography unit of the present invention are roughly analogous to those operations performed by the circuit of Yup. However, the performance of cryptographic rounds in the cryptography unit is responsive to prescription of the cryptographic operation by a single atomic cryptographic instruction provided in a program flow for execution by the microprocessor, and Yup utterly fails to teach this aspect of the present invention.

In reply to the Examiner's concession that Yup does not explicitly disclose performing these instructions on a microprocessor based platform, Applicant agrees. And moreover,

Applicant specifically notes that claim 1 does not recite a "microprocessor based platform" but rather a "microprocessor."

Consequently, in reply to the Examiner's statement that that Dhir discloses a similar apparatus and further discloses performing cryptographic instructions (i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform (i.e., FPGA), Applicant wishes to make several points. First, as noted above, claim 1 specifically recites a microprocessor, not a microprocessor based platform. It is furthermore asserted that a microprocessor is clearly disclosed within the instant specification and drawings and is quite distinct from a microprocessor based platform, which one skilled in the art will appreciate to comprise, for example, one or more microprocessors, memory, coprocessors, I/O, operator interface, etc. And while the hardware to perform cryptography is presently known to be disposed as a coprocessor, it is respectfully asserted that there is no implementation of a microprocessor that includes such capability.

Secondly, Applicant respectfully disagrees with the Examiner's characterization of Dhir's invention as a microprocessor based platform. Applicant submits that one skilled in the art would characterize Dhir's invention as a field programmable gate array (FPGA) is that is coupled to memory having programming instructions for configuring the FPGA with a medium access layer selected from more than one type of medium access layers. [Abstract – an FPGA is not a microprocessor, nor is it a microprocessor based platform.] Applicant further submits that a more correct characterization of Dhir's invention would be a FPGA-based platform.

Applicant has been careful to search Dhir and finds that a microprocessor is only mentioned twice and it is noted that fixed logic circuit 32 may be a microprocessor, which is provided to replace a set of configurable logic blocks 80, a set of memory blocks 90, and/or a set of multipliers 92, as are found in the X4000E family of field programmable gate arrays and/or the Virtex-II field programmable gate arrays. [paragraphs [0033] and [0037]]. Certainly Dhir does not teach, nor does he suggest, a microprocessor as is disclosed in the instant application and which is recited in claim 1.

All Dhir teaches is that one may replace fixed logic 32 with a microprocessor. Dhir certainly does not teach a microprocessor that fetches and executes cryptographic instructions as part of an instruction flow (i.e., an application program). Applicant provides an example of a microprocessor in the instant disclosure as an x86-compatible microprocessor. This is obviously not what is taught by either Yup or Dhir, nor can it be derived from a combination of the two references.

Regarding Yu, Applicant has carefully reviewed the teachings therein and respectfully submits that Yu teaches a mechanism for performing AES encryption that is substantially equivalent to the circuit taught by Yup. The Examiner pointed Applicant to FIGURE 7a of Yu to find support for the assertion that Yu teaches performing cryptographic instructions to implement AES on a single microprocessor. Applicant respectfully disagrees and notes that Yu teaches a dedicated cryptographic processor 700 that is coupled to a separate host processor 710 and receives instructions and data to perform AES rounds over 32-bit host busses. The cipher subprocessor employs direct memory access (DMA) techniques to perform transactions to/from the host processor's memory 851 to store/load data and instructions. Applicant notes that such a separate dedicated cryptographic "processor" approach is discussed, along with its commensurate limitations, in paragraphs 19-20, *inter alia*, of the instant specification. (Figures 8, 11, and 12, and column 8, lines 6-15)

Respectfully, Applicant stresses that the approaches of Yup, Dhir, and Yu are techniques employed by hardware *external to a microprocessor,* the disadvantages and limitations of which Applicant notes within the instant application. The apparatus of claim 1, on the other hand, performs cryptographic operations *within a microprocessor, responsive to a single atomic cryptographic instruction fetched from memory,* which is advantageous in one aspect in that an instruction is provided for use by a programmer to instruct the microprocessor to perform one of a plurality of cryptographic operations. In addition, the cryptographic rounds are performed by a cryptography unit that is within the execution logic of the microprocessor, and not by a separate unit that is external to the microprocessor.

Based upon the above arguments, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

With respect to claims 2-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup, Dhir, Yu, or a combination of the references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-15.

By this communication, claim 16 is cancelled, thereby rendering the rejection moot.

As per claim 17, the Examiner noted that Yup disclose an apparatus for performing cryptographic operations, comprising:

- a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes that a cryptographic key be expanded into a corresponding key schedule be employed when executing said one of the cryptographic operations [page 3, paragraph 0028]; and
- keygen logic (key expansion block), operatively coupled within said cryptography unit, configured to direct said device to perform said one of the cryptographic operations and to expand said cryptographic key into said corresponding key schedule [page 3, paragraph 0028].

The Examiner stated that Yup does not explicitly disclose performing these instructions on a microprocessor based platform nor performing the instruction within a single microprocessor, but that Dhir discloses a similar apparatus and further discloses performing cryptographic instructions (i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform (i.e., FPGA) [page 5, paragraph 0051], and that Yu discloses a similar apparatus and further discloses performing cryptographic instructions to implement AES on a single microprocessor.

The Examiner therefore concluded that it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a single microprocessor, a microprocessor based platform, or any other platform in order to meet particular design requirements.

Applicant respectfully disagrees with the Examiner's arguments provided above and directs attention to the arguments submitted in traversal of the rejection of claim 1. In summary, both Yup's invention and Yu's cipher subprocessor are stand-alone units, not part of a microprocessor. As such, they do not execute an instruction flow. And furthermore, the instruction flow taught by Applicant includes a single atomic cryptographic instruction that prescribes, *inter alia*, that an intermediate result be generated during execution of one of the cryptographic operations. Applicant teaches that the single cryptographic instruction is translated into a sequence of micro instructions that directs the microprocessor to perform the prescribed cryptographic operation. And Applicant's cryptographic rounds are performed by a cryptography unit that is integral to the execution logic of the microprocessor.

In addition, Dhir's invention is a field programmable gate array (FPGA) is that is coupled to memory having programming instructions for configuring the FPGA with a medium access layer selected from more than one type of medium access layers. Dhir's FPGA is not a microprocessor, nor does it teach or suggest fetch logic within a microprocessor for fetching a cryptographic instruction from memory.

In view of the above arguments, it is respectfully requested that the rejection of claim 17 be withdrawn.

With respect to claims 18-21 these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by Yup, Dhir, Yu, or a combination of the references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18-21.

As per claim 22, the Examiner noted that Yup disclose a method for performing cryptographic operations in a device, the method comprising:

- receiving a cryptographic instruction that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations and expanding the cryptographic key into the corresponding key schedule [page 3, paragraph 0028];

The Examiner noted that Yup does not explicitly disclose performing these instructions on a microprocessor based platform nor performing the instruction within a single microprocessor, but that Dhir discloses a similar method and further discloses performing cryptographic instructions (i.e., program instructions) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform (i.e., FPGA) [page 5, paragraph 0051], and that Yu discloses performing cryptographic instructions to implement the AES algorithm on a single microprocessor.

The Examiner therefore concluded that it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a single microprocessor, a microprocessor based platform, or any other platform in order to meet particular design requirements.

Applicant respectfully disagrees with the points asserted above and directs the Examiner's attention to the arguments submitted in traversal of the rejections of claims 1 and 17. Claim 22 recites, among other elements and limitations, within a microprocessor, fetching and translating a single atomic cryptographic instruction—not instructions, plural—from memory that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations. As noted earlier, neither Yup nor Yu teach a microprocessor, nor it is taught that the microprocessor receives a single atomic cryptographic instruction that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations. This is because Yup and Yu teach a stand-alone AES unit that is fed data from system channels. In addition, Dhir teaches using FPGAs to configure a MAC layer device on a wireless LAN. Neither Yup, Dhir, nor Yu teach or suggest fetching a single atomic cryptographic instruction from memory that prescribes expansion of a cryptographic key into a

corresponding key schedule for employment during execution of one of a plurality of cryptographic operations, and via a cryptography unit disposed within execution logic in the microprocessor, expanding the cryptographic key into the corresponding key schedule.

Accordingly, it is respectfully requested that the rejection of claim 22 be withdrawn.

With respect to claims 23-26, these claims depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Yup, Dhir, Yu, or any combination of the two references Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 23-26.

RECEIVED
CENTRAL FAX CENTER
MAR 07 2008

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-15 and 17-26 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

By: /Richard K. Huffman/

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

Date: 03/07/2008

PAGE 27/29 * RCVD AT 3/7/2008 11:10:00 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-5/39 * DNIS:2738300 * CSID:661 460 1986 * DURATION (mm-ss):07-34